

POC DMZ - Rapport de mise en service

Table des matières

POC DMZ - Rapport de mise en service

Table des matières

Schéma de l'infrastructure

User Story 1

User Story 2

User Story 3

User Story 4

User Story 5

User Story 6

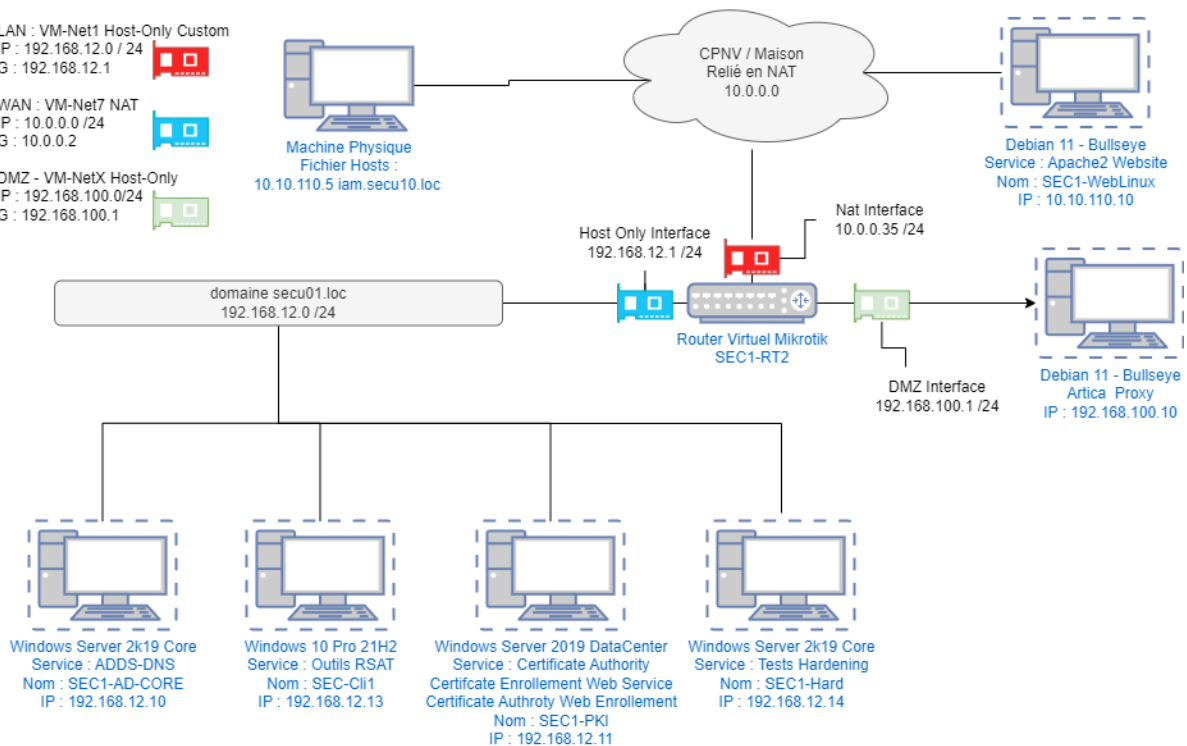
Schéma de l'infrastructure

Networks

LAN : VM-Net1 Host-Only Custom
IP : 192.168.12.0 / 24
G : 192.168.12.1

WAN : VM-Net7 NAT
IP : 10.0.0.0 / 24
G : 10.0.0.2

DMZ - VM-NetX Host-Only
IP : 192.168.100.0 / 24
G : 192.168.100.1



User Story 1

En tant qu'utilisateur du LAN j'aimerais accéder à Internet de manière sécurisée dans le but de ne pas compromettre la sécurité de mon entreprise.

- Copie d'écran de la config du proxy dans le navigateur

Proxy

Configuration manuelle du proxy

Utilisez un serveur proxy pour les connexions Ethernet ou Wi-Fi. Ces paramètres ne s'appliquent pas aux connexions VPN.

Utiliser un serveur proxy

☒ Activé

Adresse

192.168.100.10

Port

8080

Utilisez le serveur proxy sauf pour les adresses qui commencent par les entrées suivantes. Utilisez des points-virgules (;) pour séparer les entrées.

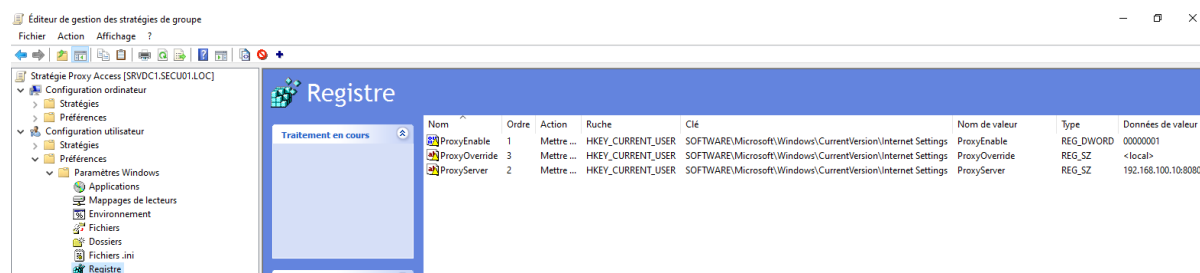
☒ Ne pas utiliser le serveur proxy pour les adresses (intranet) locales

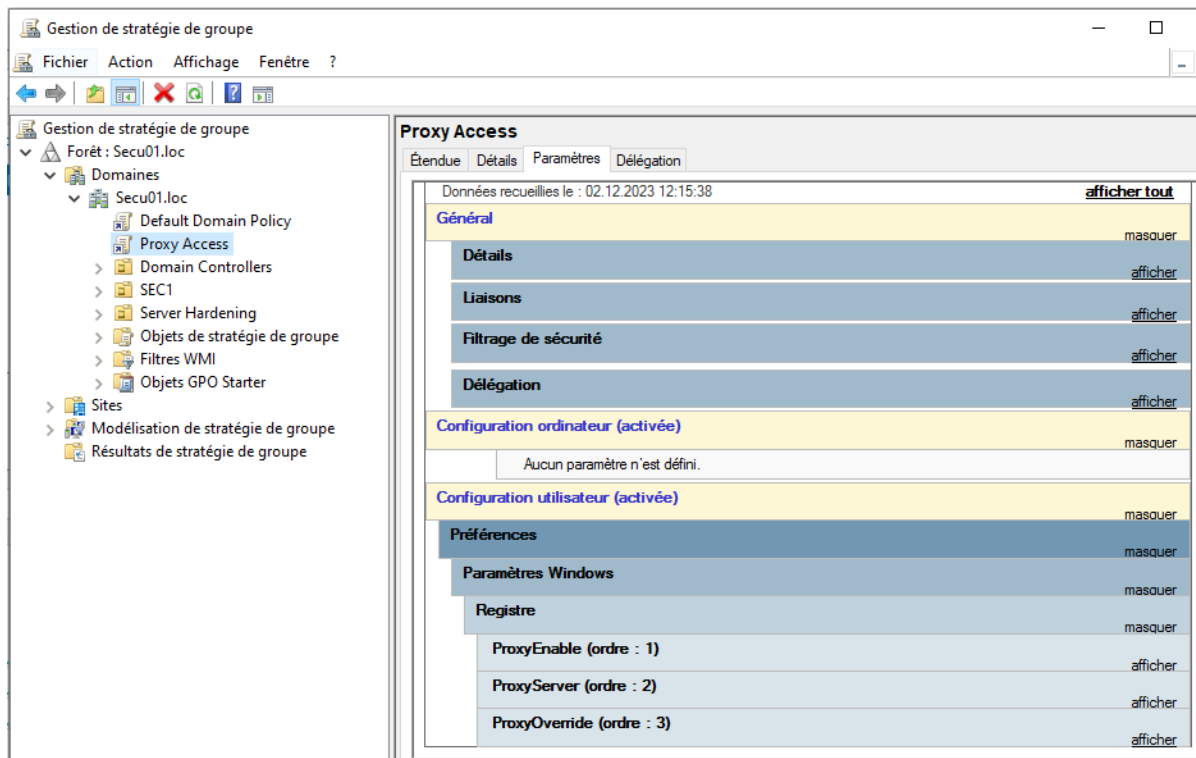
Enregistrer

User Story 2

En tant qu'utilisateur du LAN j'aimerais que mon navigateur soit configuré de manière automatique au niveau du proxy à utiliser, dans le but de se simplifier la vie.

- Copie d'écran de la GPO, proxy.pac ou autre config
- <local> dans override modifié par "192.168.12.*" lors de la config de radius





User Story 3

En tant que responsable de la sécurité, j'aimerais que les machines de mon infrastructure puissent communiquer en respectant les principes d'une DMZ, dans le but de sécuriser mon infrastructure contre la compromission d'une ou plusieurs machines.

- [Tableau des règles du firewall](#)

Source	Destination	Protocol	Action
LAN	Any	Any	Block
LAN	DMZ	8080 (SquidProxy)	Pass
DMZ	WAN	443 (HTTPS)	Pass
DMZ	LAN (192.168.12.11)	1812 (RADIUS)	Pass
WAN	DMZ (192.168.100.10)	80 (HTTP)	Pass

User Story 4

En tant que CTO, j'aimerais que les utilisateurs du LAN puissent surfer sur un nombre restreint de sites (www.cpnv.ch, www.vd.ch), pour améliorer leur productivité.

- [Caputre d'écrans : config squid et test accès depuis le cli1 à vd.ch et youtube](#)

- [Parfois la page d'erreur squid s'affiche parfois non et c'est juste une page d'erreur google](#)

```
cpnv@srvprxy: /etc/squid/conf.d
cpnv@srvprxy:/etc/squid/conf.d$ cat sec2.conf
http_port 192.168.100.10:8080
cache_dir ufs /var/spool/squid 100 16 256

#acl lannet src 192.168.12.0/24
#acl dmznet src 192.168.100.0/24
acl whitelist dstdomain "/etc/squid/conf.d/sites.whitelist.txt"

#http_access allow lannet
#http_access allow dmznet
http_access allow whitelist

http_access deny all
cpnv@srvprxy:/etc/squid/conf.d$ cat sites.whitelist.txt
.google.ch
.vd.ch
.cpnv.ch
cpnv@srvprxy:/etc/squid/conf.d$
```

Site officiel du Canton de Vaud | x +

vd.ch

Site officiel
ÉTAT DE VAUD

AFFICHER LES THÈMES +

ACTUALITÉS

ERREUR : l'URL demandée n'a pas pu être trouvée

Non sécurisé | youtube.ch

ERREUR

L'URL demandée n'a pas pu être trouvée

L'erreur suivante s'est produite en essayant d'accéder à l'URL : <http://youtube.ch/>

Accès interdit.

La configuration du contrôle d'accès, empêche votre requête d'être acceptée. Si vous pensez que c'est une erreur, contactez votre administrateur proxy est [webmaster](#).

Générée le Sat, 02 Dec 2023 11:19:34 GMT par srvprxy (squid/5.7)

Administrateur : Invite de commandes

Microsoft Windows [version 10.0.19045.3693]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet0 :

Suffixe DNS propre à la connexion. . . . :
Adresse IPv6 de liaison locale. . . . : fe80::f4a0:6d59:23ae:a444%16
Adresse IPv4. : 192.168.12.13
Masque de sous-réseau. : 255.255.255.0
Passerelle par défaut. : 192.168.12.1

C:\Users\Administrateur>whoami
secu01\Administrateur

C:\Users\Administrateur>hostname
CLI1

C:\Users\Administrateur>

User Story 5

En tant que responsable de la sécurité, j'aimerais que le LAN puisse accéder au WAN uniquement à l'aide de ping et protocoles web (https, http), dans le but de protéger l'infrastructure

- Accès only au ping, ping 8.8.8.8 passe mais sur le web only vd.ch
- Depuis CLI1, ping 8.8.8.8 ok avec accès aux sites voulus mais pas aux autres

The screenshot shows a multi-monitor environment with the following content:

- Top-left monitor:** A web browser displaying a 404 error page for `youtube.ch`. The error message is "ERREUR L'URL demandée n'a pas pu être trouvée". It includes details about the failed request to `http://youtube.ch/` and mentions an "Accès interdit" (Access denied) status.
- Bottom-left monitor:** A Windows command prompt window showing the output of `ipconfig` and `ping 8.8.8.8`. The IP configuration shows a local IPv6 address and a local IPv4 address (192.168.12.13). The ping results show successful connectivity to 8.8.8.8 with a TTL of 127.
- Top-right monitor:** A web browser displaying the CPNV (Centre professionnel du Nord vaudois) website. The site has a navigation menu with "LE CPNV", "FORMATIONS", and "ADMISSION". The main content area features a banner for "Ensemble, développons votre" and a "FORMATIONS" button.
- Bottom-right monitor:** A web browser displaying the official website of the Canton of Vaud (Site officiel du Canton de Vaud). The site features a "ÉTAT DE VAUD" section with a button to "AFFICHER LES THÈMES".

User Story 6

En tant que responsable informatique, je veux que les internautes puissent avoir accès à un site web dans le DMZ qui réponde à `http://iam.secuxx.internal`, dans le but de par la suite mettre en place un service d'authentification.

- Machine ajoutée - Client windows dans le NAT, problème avec opnsense pour sortir sur pc physique, accès et règles OK pour WAN mais pas pour pc physique

